FEDERAL TRADE COMMISSION

I N D E X

FEDERAL TRADE COMMISSION

In the Matter of: )
REPORT TO CONGRESS PURSUANT )
TO CAN-SPAM ACT. ) Matter No. P044405
----------)

MONDAY
FEBRUARY 23, 2004

Room 432
Federal Trade Commission
6th and Pennsylvania Avenue, NW
Washington, D.C. 20580

The above-entitled matter came on for conference, pursuant to agreement at 1:05 p.m.

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:

COLLEEN ROBBINS
DAN SALSBURG
SHERYL DREXLER
JULIE BUSH
Federal Trade Commission
6th and Pennsylvania Avenue, NW
Washington, D.C. 20580

PARTICIPANTS (VIA TELEPHONE):

JON PRAED
DAVE KRAMER

P R O C E E D I N G S

MS. ROBBINS: Today is Monday, February 23, 2004. It is approximately 1:05 Eastern Standard Time, and we're meeting today with Jon Praed and David Kramer. They are participating by phone to discuss a possible National Do Not E-Mail Registry and the reward system.

This meeting is being transcribed by a court reporter who does not have the benefit of seeing you in person, so at least in the beginning, if you could identify yourself before you speak, so the court reporter will accurately take down who is saying what.

My name is Colleen Robbins. I'm an attorney with the Federal Trade Commission's Division of Marketing Practices, and I'm here today with Dan Salsburg, Sheryl Drexler, and Julie Bush. Jon and David, if you could just identify your affiliations please.

MR. PRAED: Sure. I'm Jon Praed with Internet Law Group in Arlington, Virginia.

MR. KRAMER: And I'm Dave Kramer with Wilson, Sonsini, Goodrich, and Rosati in Palo Alto, California.

MS. ROBBINS: Just by way of background, Section 9 of the CAN-SPAM Act directs the Commission to prepare a report that has to outline a plan and a timetable for establishing a Do Not E-Mail Registry. The report must also describe any technical, practical,

security, privacy, or enforceability concerns the Commission may have with such a Registry. This report also must include information on how such a Registry would affect e-mail accounts. In addition, we have to prepare a report on a bounty reward system.

In preparation for drafting the Do Not E-Mail Registry report, we're collecting information from as many sources as possible in a very short amount of time. The report to Congress is due on June 16, 2004, and to help us facilitate this, the statements that you make today may be cited in the report to Congress. That's one of the reasons why we are transcribing this discussion.

A Do Not E-Mail Registry could take several different forms, and to start off with, I'd like to get your thoughts on a Do Not E-Mail Registry that would be based on the Do Not Call model. Consumers would register their e-mail addresses in a central database, e-mail marketers would then scrub their lists and send their e-mail only to those people who are not on the database.

MR. KRAMER: Sure. This is Dave Kramer. I think that, at bottom, that's absolutely necessary for any sort of effective spam legislation, barring a prohibition, which I think some of you know I am in favor of.

A Do Not Spam centralized Registry where a

consumer can place his or her e-mail address on a list and know, at that point forward or from that point forward, that any future message sent to that consumer to which a consumer has not expressly consented is a violation of the law, is a necessity for any sort of effective anti-spam program.

The concern that I have is in enforcement of a Do Not Spam Registry.

I know that -- I have heard, at least, the FTC express concerns about consumer expectations with respect to a Do Not Spam List. I am personally, and know of many others who have been, wildly impressed with the success of the Do Not Call List, and understandably, I think the Commission is concerned that consumers will have false expectations in light of the Do Not Call experience if the FTC implements a Do Not Spam List. Consumers will expect spam to disappear almost overnight, the way that telemarketing calls appear to have disappeared.

So, I think that -- obviously, the issues of enforcement and consumer expectations are paramount there. But a centralized list through which spammers or e-mailers or direct marketers will scrub their own e-mail list is the way to go.

I think there are some technical issues involved, particularly with respect to whether or not

direct marketers actually get access to the names on the list, which they do in the Do Not Call scenario. That's certainly something that needs to be worked out, but in concept and in principle, the Do Not Spam List is essential.

MR. PRAED: Colleen, you suggested that there were three basic models. I'm not familiar with the trilogy you discussed, so before I get too deep into any one -- I don't want to repeat myself -- let me just generally say I think the idea of a Do Not E-Mail List is workable.

All of the concerns David outlined, I would echo, as well, particularly -- my main purpose in participating today is to try to provide you some insight on enforcement. I think, obviously, any Do Not E-Mail List will require some enforcement. And a couple of thoughts at a broad scale. One is I think the success that you're seeing with the Do Not Call List may or may not last. As that call list -- as the impact of the Do Not Call List becomes fully known to the telemarketing community, I think you may find the telemarketing community taking steps to arrange their businesses so that the Do Not Call List does not impact their work as greatly as it currently is.

For example, you may see offshore telemarketing

companies opening up that -- and I'm not an expert on the Do Not Call List, but it strikes me you may see, generically stated, a general movement offshore in the telemarketing business in an attempt to find a way to -- I don't want to say evade, but to get around appropriately the scope of the Do Not Call List, and I think that we're going to see the same sort of thing with any Do Not E-Mail List.

The problem with the Do Not E-Mail List that will make its impact immediately less apparent than the Do Not Call, I believe, is that so many people who are engaged in spam today are what I think David and I frequently refer to as "simply criminals." They are not traditional, well-established businesses that are predominantly the norm in the telemarketing business. People who are sending spam professionally today, unsolicited commercial e-mail, are largely engaged in fly-by-night enterprises where they're simply looking to make a quick buck and are not looking to raise consumer awareness of their brand or any other long-term business interest.

MR. SALSBURG: Would a Do Not E-Mail Registry actually have much of an impact on the amount of spam in consumers' inboxes?

MR. PRAED: Well, I think that it could. I

think it will do two things that could be valuable.

One is it could provide consumers with a facial way to know what legitimate mail they're receiving as distinct from illegitimate mail. And it also could provide the FTC or some other government entity with a useful enforcement mechanism, a useful statutory mechanism that they could hinge enforcement actions against, so that your proof, if you will, is simply that someone whose name was on the list received a commercial e-mail, and that could simplify your proof and allow you to quantify complaints in ways that you currently can't quantify because the legal actions that you're allowed to take are not made simply on the mere fact that a commercial e-mail was sent to a recipient whose name was on the list after a point in time when their names got added to the list and disseminated.

So, I think it provides you opportunities for consumers, when they look at their inbox, to see e-mail that they know is patently violative of some Federal law, and two, it provides you a different and, in some ways, superior enforcement mechanism to take action against those people who are doing that.

But I think both -- and it's interesting to me to see how effective the Do Not Call List has been, and I am somewhat intrigued that -- and I don't want to say

telemarketers are honoring it -- I don't want to say I'm surprised by that, but I guess I'm surprised that there are not more creative attempts being made by the telemarketing industry to find ways to lawfully continue to make calls without being affected by the list, and I have not looked at the international implications of the list, but that strikes me as one place you're likely to see telemarketers looking in the future.

So, you may see the effectiveness of the Do Not Call List being diminished if the economics of that sort of business model are there. Again, I don't know the full details of that, but I think you may see some convergence between the effectiveness of the two types of lists.

MS. ROBBINS: Jon, you said that you may have some insight on enforcement with a central registry. Could you just elaborate on that?

MR. PRAED: Well, I think any statutory mechanism that is put in place to prohibit spam or -- when I say spam, I mean unsolicited commercial e-mail -- is going to require an enforcement mechanism. Good companies will always, I believe, try to follow the law, but there is so much money to be made through spam that people who are not deterred by simple -- the simple passage of a law -- aren't going to be deterred by the

CAN-SPAM Act or a Do Not Spam Registry.

Indeed, I think you will find some people who will e-mail people on a Do Not Spam List advertising particular types of products that those people might be generally viewed as more likely to buy. For example, anti-spyware or other sorts of privacy products might find themselves the subject of those sorts of spam messages, because they've indicated to the public that they would prefer to be left alone.

So, you're always going to need some enforcement mechanism so that people who are either injured by the transmission or the government can take action against people who are doing that. Without that sort of enforcement mechanism, I think many laws are going to be fairly toothless. That goes well beyond a Do Not Spam List.

MR. SALSBURG: What extra punch does a Do Not E-Mail List have for enforcement compared to the government's ability to enforce the opt-out requirements currently required by CAN-SPAM?

MR. KRAMER: Jon, do you want to speak to that, or would you like me to pick it up?

MR. PRAED: Yeah, if you want to --

MR. KRAMER: Sure. To reiterate Jon's point in summary fashion, it's a very easy way for a consumer to

know, upon receipt of a message, that the message was sent in violation of the law, and it's an easy way for the FTC, or whomever the government's enforcement agency is, to recognize that there has been a violation of the law. They can simply check to see whether the consumer's name is on the List and, if it is, compare that with the receipt of the message or the message that was received and recognize that there was a violation.

So, I do think it's somewhat easier to make out a prima facie case of a violation if there is a Do Not Spam List. But I think that the question assumes that a Do Not Spam List would need to be enforced under the current enforcement mechanism that CAN-SPAM sets up, and I'm not sure that that's the case.

I think the CAN-SPAM Act gave the FTC wide-ranging authority to make recommendations about what the enforcement mechanism ought to be, and I think -- and I'll leave it to Jon to express his views on this, but I think that it's perfectly within the FTC's purview to recommend a private right of action for violation of the Do Not Spam List, and I think the FTC absolutely needs to do that.

I think that CAN-SPAM's biggest shortcoming is a lack of effective enforcement. Unless the legislation builds into it some form of private right of action which

gives aggrieved consumers the ability to take action on their own behalf for statutory damages so as to create general deterrence and create a real threat of economic harm to the perpetrator, I think CAN-SPAM and, ultimately, a Do Not Spam List are not going to be successful.

MR. PRAED: I would echo most of that. I would say I think a private right of action that empowers individuals is, in the end, not going to be a good result. I think everyone is in favor of empowering the individual consumer to take some action, but I think there needs to be a focus on the -- what sort of action a consumer can realistically take to actually identify and stop spammers, and from my experience in suing spammers -- identifying them and suing them on behalf of some major ISP's, I am convinced that it takes, in almost every case, too much work to identify a spammer for a consumer to realistically be expected to invest that sort of resource. We may get to this on the reward question, as well.

Most spammers, by the time you catch them, don't have much left in the way of resources, and getting -- using spammer resources as a mechanism for funding the enforcement mechanism is unlikely to be successful. So, to say that an individual consumer could find a

traditional plaintiff lawyer who, on a contingency-fee basis, would sue a spammer I think is pretty unrealistic.

If your hope is that that sort of an enforcement mechanism is actually going to target truly culpable and high-volume spammers, illegal criminal spammers, if you create such a mechanism, I think the only thing -- the only -- the biggest impact you will find is that consumers and contingency-fee lawyers will look for opportunities to sue deep pockets because of a snafu in a deep-pocket company's mailing practices, and while some may argue that that's a good thing, I think that that's a completely different situation from the problem that I focused on, which is really fraudulent criminal spam.

MR. KRAMER: Right. So, Jon and I would agree on most of the issues here, but it's on this point where I think we disagree.

I think that, from a consumer's perspective, it doesn't matter whether a spam that's sent to them is sent by a irreputable or disreputable fly-by-night organization or a large multi-national conglomerate. The message has exactly the same impact. It's equally disruptive. It's equally unwelcome. It's equally uninvited. And as a result, the consumer should be entitled to make the choice as to whether or not to go

after whomever is sending those messages.

Whether it's the result of a internal company snafu or not, the messages are still problematic. They cause just as much burden on the ISP. They cause just as much burden to the consumer to deal with.

So, while I certainly agree that spammers that engage in fraudulent and otherwise criminal conduct ought to be subject to different and higher penalties, I think what we're talking about here is the problem of spam generally, and singling out criminal or fraudulent spammers to suggest that that really is the problem, I think, understates the problem. There are a host of companies, and there will be increasing numbers of companies, who are interested in utilizing the mechanisms of commercial e-mail and unsolicited commercial e-mail to market their wares that you and I would not consider to be disreputable.

MR. SALSBURG: Okay. Why don't we move on to another possible model that some have floated out there for a Do Not E-Mail Registry, and that's a domain wide opt-out registry where an ISP or a business that's a domain owner could register the entire domain, all e-mail addresses on the domain, with the Registry, and then e-mail marketers would have to scrub their lists to remove any e-mail addresses that appear at those domains.

MR. KRAMER: And does the system make allowances for consumer preferences and consumer choice to override the ISP's or the domain owner's preferences?

MR. SALSBURG: Yes, let's assume that an individual consumer who has an e-mail account from an ISP can then opt back in to receive unsolicited commercial e-mail.

MR. KRAMER: Okay. That's precisely the system that we had envisioned here in California, drafted in California Business and Professions Code 17538.45, allowing for domain wide opt-out. We actually floated the idea of a centralized Registry where domain owners could list their domains, but for whatever reason, Governor Davis did not sign that additional amendment into law.

I think it's a great idea. I think it deals with the issue that Jon and I are debating over very clearly. It says we are going to put power of enforcement in the hands of the domain owners who are going to hopefully have adequate -- I shouldn't jump ahead -- I'm not sure that you are contemplating a world in which the domain owners would have the enforcement power in the event that they put themselves on the list, but certainly they would need to for that list to be effective, and they certainly would have greater

resources than your average consumer to take action.

The one caveat there would be that, in order to make it an economically viable proposition for a domain owner, there would need to be statutory damages and certainty as to what the economic recovery would be in a litigation.

The current statute, which allows for statutory damages of up to $25 or up to $100 is flawed in that respect. An ISP can't decide, going into litigation, what the expected recovery is going to be, because the question of what the -- of the per-message statutory damages is left to the court's discretion. That's simply not appropriate in this context.

MR. PRAED: If I could comment, as well, on David's concern about empowering consumers, I had originally suggested empowering them to bring suit, in my view, is not a viable option for most consumers. I think there are ways that consumers can be empowered, though, but I think it need -- they need to be empowered to do things that are less burdensome for them than the filing of a lawsuit and prosecuting it through to judgement and then trying to actually collect on the judgement.

I think you're going to find that that -- empowering them with just that tool and that tool alone is -- while some consumers may applaud it in theory,

you're going to find that very few consumers, if any, actually can do it, and I think there are some alternatives ways that can be empowered that, in the end, will provide them with more meaningful opportunities to participate in the really specific way. I floated this idea before at a couple of the conferences where I've talked.

I know a lot of people -- let me summarize it briefly, in maybe 30 seconds, for you. One thing that consumers need is transparency in the e-mails that they receive.

I know a lot of people have talked about imposing a labeling requirement on commercial e-mail, and there's a lot of dispute about whether that is workable or appropriate or fair for commercial seekers to be required to put such a label in place.

My proposal comes down to the -- builds on the concept of a label but a label that adds value. So, it is not simply an ADV label or any sort of a -- in a sense -- a negative label. I think most bulk mailers oppose the idea of labeling, because they view it as simply a requirement that they put what is viewed, in essence, as a negative statement in their e-mail message.

Rather, my idea of a label is one that adds value, that I think, if adopted, you would find

commercial mailers embracing, which is the idea of putting in a disclosure that records the identity of the custodian of record for that mailer, who has the records on file that memorializes the consent that the recipient gave that justifies the e-mail. The model that I built this on is the -- there's a statute, 18 U.S. Code --

MR. KRAMER: The adult porn statute.

MR. PRAED: It's the adult model age of consent statute that requires all persons who display adult performances attach to those performances a disclosure of custodian record, who basically has photocopies of all the models' -- all the performers' driver's licenses establishing they were over the age of 18.

My proposal is that that sort of a disclosure be contained within all commercial e-mail providing the consumer with the name of a person in the United States, a phone number, an address, an e-mail address that they can use to immediately reach out to someone and say, "Show me my 3-by-5 card in your file. What is it that you have in your possession that caused you to send me this e-mail? What do you have that you claim I did that justifies you e-mailing me this," and that -- there are some details to that that I think need to be considered to make it workable, but the idea is to provide consumers with something they can look for in the e-mail itself

that, if it's there, they can take action very quickly and easily. They can pick up the phone and make a phone call, and if nobody picks up that phone or it's constantly busy or the phone number doesn't work, they immediately know this e-mail is in violation of that Federal law.

MR. SALSBURG: Let me throw out a third possible model --

MR. PRAED: Okay.

MR. SALSBURG: -- and that's that of a third-party e-mail forwarding service. Under this model, the actual list of consumer e-mail addresses would be held by a, or a number of third parties that would not be actual e-mailer marketers. Instead, e-mail marketers would submit their marketing lists to these third parties, which would then scrub and send the messages.

MR. KRAMER: I actually harkened to that in my opening remarks about the concern that you'd be giving the fox the keys to the hen house if you allowed people to buy the lists the way that they are bought in the Do Not Call scenario. I think that makes sense, but I think all of these plans break down on the question of enforcement and who we're going to empower to enforce.

Just to follow up on 17538.45, which was California's attempt at this domain wide opt-out system,

the reason that California's system did not work was, at least in my mind, because the economics created by the statute were insufficient to create an incentive for suit.

The statute in California empowered people -- ISP's, domain owners -- to sue for $50 a message but capped recovery at $25,000 a day. As a result, it didn't create sufficient economic incentive for an ISP to incur the attorney's fees and litigation costs associated with litigation, because the up-side just wasn't there.

That, coupled with the fact that, in many cases, the people sending these messages are almost certainly judgment-proof, was essentially the death knell to the legislation. There have been only a handful of suits brought under that statute.

I think if you're going enact a domain wide opt-out system, what you need to create are sufficient economic incentives for litigation, statutory damages that have a floor, not a ceiling, and the potential for recovering attorneys' fees. If you have that, I think you'll see far greater enforcement than we saw in California.

MR. SALSBURG: Jon, do you have any thoughts on the third-party forwarding service as a model for a Do Not E-Mail Registry?

MR. PRAED: Yeah, I do, two thoughts. One, I think you need to be concerned about setting up third parties to be used as e-mail forwarding. It strikes me that, unless you have a good grasp on the volume that you're talking about, it could well be difficult for essentially all commercial e-mail to go through these forwarding entities, and I think you get into a fairly intense regulatory question of creating sort of a monopoly power.

I think the solution, though, is in technology. I think there are some technological fixes where you can have a government-maintained database, a central database that marketers would have to scrub their list against and run in a way that does not allow marketers to be able to know what names have been removed from the list. I know that technology exists.

I know of at least one company that's working in that space, a company called “unspam” and that strikes me as really the best way to run that sort of a program, because it provides you with, in essence, the central database but without the transparency that you're concerned about with marketers essentially getting access to that full central database.

MR. KRAMER: Right. You weren't suggesting that the messages would actually be forwarded through

that service, were you, because I echo Jon's concerns about that. I think scrubbing lists through a central service makes sense, but actually forwarding the mail through that service, I think, is not technologically feasible.

MR. SALSBURG: Okay. Let's move on to a fourth possible model, and that would be a Registry of authenticated senders. Under this model, an e-mail marketer would register with the Commission, obtain a registration number, which would have to be put into the header information of all of the commercial e-mail they sent, and they'd also have to register their IP addresses and domains where they'd be sending e-mail from. ISPs and other domain owners who receive e-mail could have access to these databases and adjust their filters to only permit commercial messages from such authenticated senders.

MR. PRAED: I'd want to think about that.

MR. KRAMER: So would I.

MR. PRAED: I don't have an immediate reaction to it.

MR. SALSBURG: Okay.

MR. PRAED: My immediate thought is I'm looking for a way that spammers could falsify or forge the information.

MR. SALSBURG: Well, let's presume that there was a way where it could be done in a fashion where it couldn't be forged.

MR. PRAED: If you come up with a solution that's unforgeable, that's a nice solution, but if it's based on a IP address, it's basically a list -- it's a proposed whitelist, in other words, where you would hold up a list of IP addresses and be suggesting to the mail-receiving community that they ought to essentially whitelist their mail servers to receive mail from that list.

MR. SALSBURG: Well, I think we'd be saying these are senders who are likely to be who they claim to be, and ISP's could take that information and use it however they want.

MR. PRAED: And you're saying because the FTC has certified these entities, the receiving mail servers should give strong consideration to also -- to whitelisting them.

MR. SALSBURG: Well, not necessarily. What we're saying is that there could be a Registry of senders who have been authenticated. That data could be made available to ISP's for whatever purpose they want to use them for.

MR. PRAED: The only apparent purpose is they'd

want to -- you know, if they believe that that's, in fact, a good list of good mailers, they would want to design their filters to recognize those mailer locations.

The problem, though, you're going to have is that you're going to have good mailers who are going to ask to be put on your list that you'll look at, and you'll do as much diligence as you can on them, and you'll put them on the list, but unbeknownst to any of you, other bad mailers are also going to get access to those IP addresses, because you're basically suggesting that direct marketers who use a particular third party to send their mail -- a lot of weight's going to be put on the integrity of that third-party mailer.

And if a direct mailer is sending mail from a location that other mailers have access to, you're now asking the receiving mail community to trust that IP address for reasons -- because one of the mailers coming from it is considered a white hat when there may well be others who are not white hats also coming from it.

MR. KRAMER: And you also create a situation in which consumers may not be able to access mail from non-whitelisted sources who simply don't know about the list or haven't taken the steps or are unwilling to take the steps to put themselves on that list.

MR. PRAED: As I say, I'm largely just reacting

-- I have not given this much thought, but the idea of a Registry of authenticated mailers is going to be fairly regulatory-intensive, it strikes me, and not technically -- it's not an obvious technical solution to me. I see a number of technical problems.

MS. ROBBINS: Do either of you have any other thoughts about any of these models or any other models that you may have thought about yourself?

MR. KRAMER: Just in terms of the nitty-gritty here, I think once you create a proposal for Congress, it ought to include some things like presumptions, evidentiary presumptions, so that, again, the consumer's task or the ISP's task or the FTC's task can be streamlined in litigation, so that there's a presumption that a message was unsolicited if the consumer's name was on the list.

That seems straightforward, but since it's the consumer, ISP, or FTC as the plaintiff in that case, it might be up to the consumer or whomever, the enforcer, to prove that the message was uninvited or unsolicited, when, in fact, I think it ought to be the other way and you ought to make that express proposal to Congress as an evidentiary matter.

MR. PRAED: I would only add that I would encourage the FTC to look at some of the litigation cases

that have been filed recently, I think in particular in the State of Utah, where consumers have been empowered to bring private causes of action, and I think you will see some of the concerns that I had raised rearing their head in some of those cases, where you found -- or I found, when I looked at those, a lot of litigation energy was being spent focusing not on what I think is 90 percent of the problem of spam but, rather, on fairly isolated cases of deep pockets being sued by individuals on a class action basis.

And it's that sort of empowerment of consumers that I think would not, in the end, be helpful in resolving the spam problem and could, in many ways, distract from what I think is the real need for top-level private party rights of action, where you need any private parties who have a broad base of information and resources necessary to go after spammers, coupled with government enforcement action, and where individuals are empowered not so much to bring suits directly but, rather, to provide information to those government and non-government actors who can bring action but also provide them with enough information so that they can make inquiries of those people sending the mail to get more information from those mailers about the basis for the mailing.

You know, it's very easy -- I would look for ways to empower consumers to be able to make phone calls and send e-mails that are meaningful, that have some legal impact or some factual impact in their lives, but don't simply give them something where all they can do is file a lawsuit, because they just -- they won't be able to pursue it to completion.

MR. KRAMER: Two more thoughts, Colleen. One is, in any Do Not Contact system, I think, misuse of the names or numbers or e-mail addresses on the list ought to result in criminal penalties. If consumers are to trust this list, they need to know that their names on it will not be misused, and I think a severe sanction ought to be in order in the event that someone misuses the information on that list.

And as to Jon's point about private rights of action, let me say that the statute in Utah was abused, but it was very poorly drafted. We have a fax statute in this country, the Telephone Consumer Protection Act. I know you all are familiar with it. The private right of action under that statute has been used effectively for 15 years and has dramatically reduced in the incidence of junk faxes in this country. So, I think it's unfair to look at Utah to decide what a private right of action ought to look like.

I think they drafted the statute badly, and I think two plaintiffs' firms in Utah abused it, but that doesn't mean that private rights of action won't work in this context, and as an analog, just look at the junk fax law in contrast to what we have with e-mail.

MS. ROBBINS: I don’t think we have any further questions for this portion of the call regarding a Do Not E-Mail Registry. We have two FTC attorneys here, Julie Bush and Michelle Chua, who would like to ask you some questions about your -- thoughts on the reward system. So, I'll turn this over to them. Thank you very much for your time. We appreciate you speaking with us.

MR. KRAMER: Sure.

MR. PRAED: Our pleasure.

DOCKET/FILE NUMBER: P044405

CASE TITLE: DO NOT E-MAIL REGISTRY MEETING

HEARING DATE: FEBRUARY 23, 2004

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED:

TAMARA SHIPP

**C E R T I F I C A T I O N O F P R O O F R E A D E R**

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SARA J. VANCE

1